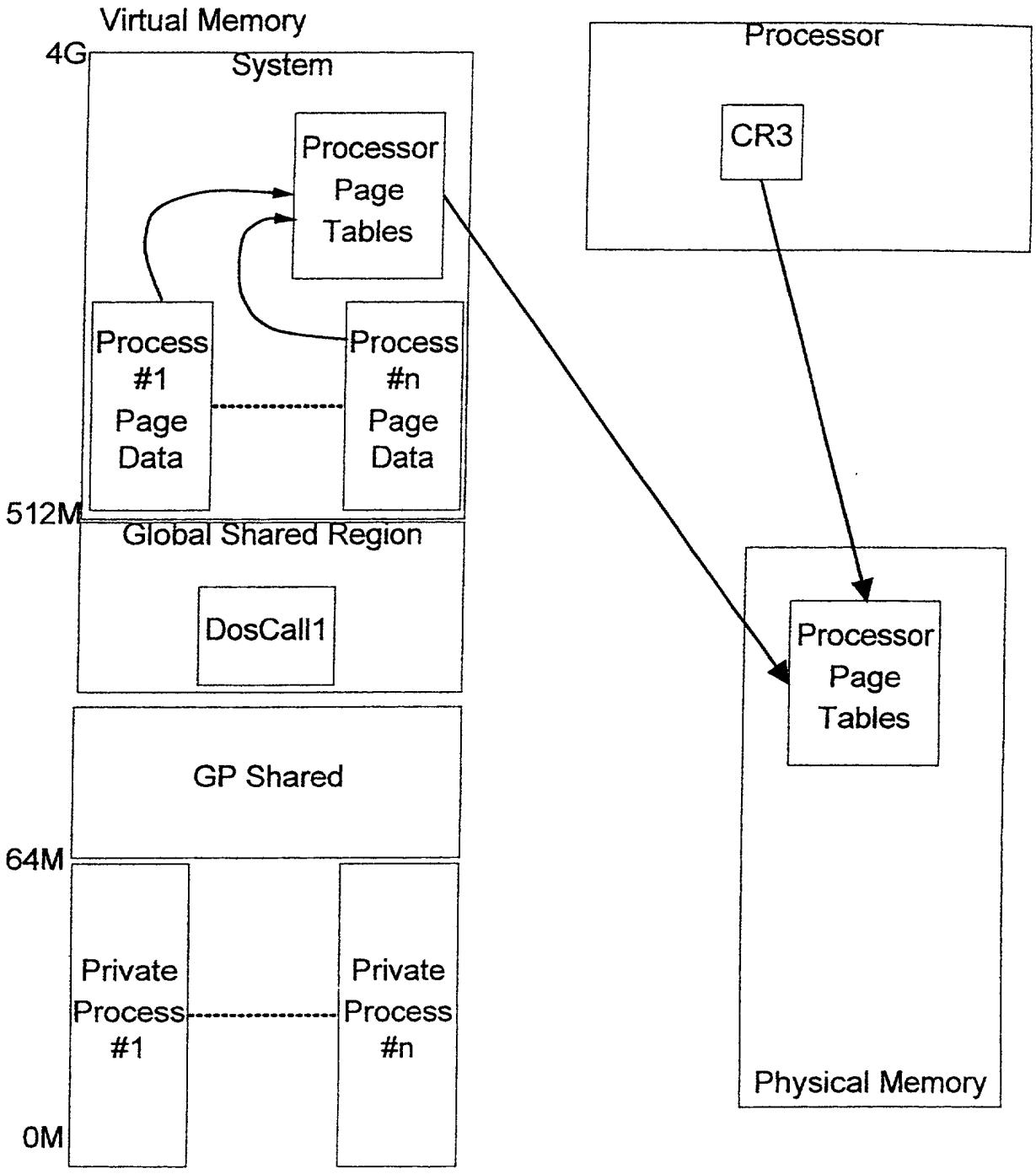
Virtual Memory
4G
System
Processor
Page
Tables
CR3
Process
#1
Page
Data
Process
#n
Page
Data
512M
Global Shared Region
DosCall1
Processor
Page
Tables
GP Shared
64M
Private
Process
#1
Private
Process
#n
Physical Memory
0M

Figure 1

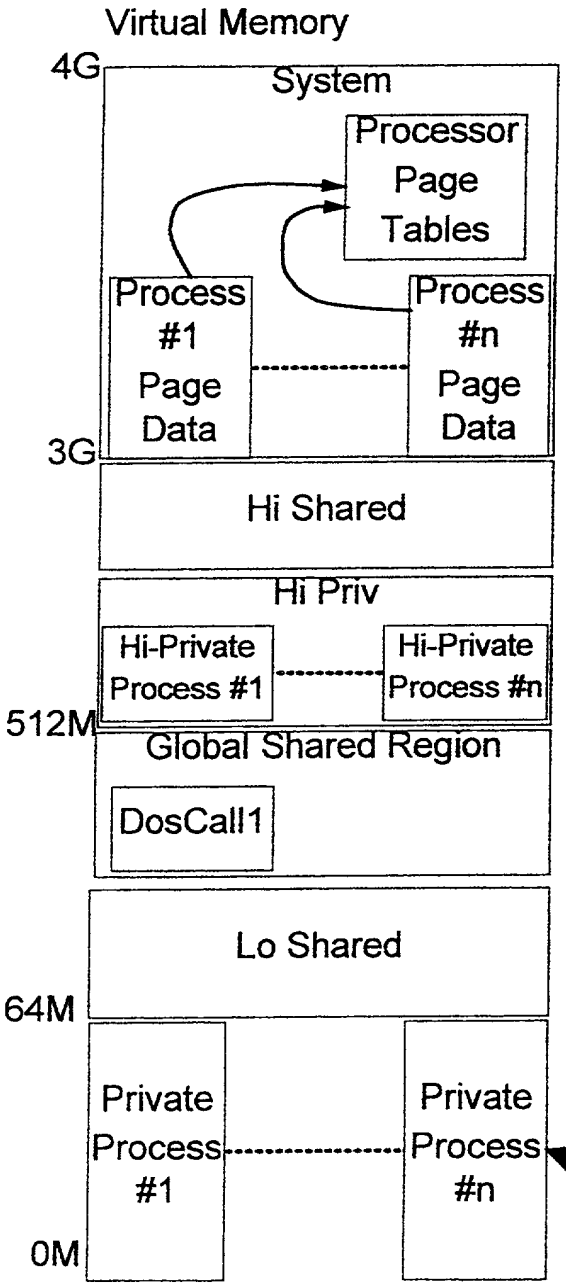
Virtual Memory
4G
System
Processor Page Tables
Process #1 Page Data
Process #n Page Data
3G
Hi Shared
Hi Priv
Hi-Private Process #1
Hi-Private Process #n
512M
Global Shared Region
DosCall1
Lo Shared
64M
Private Process #1
Private Process #n
0M
Lo Priv

Figure 2

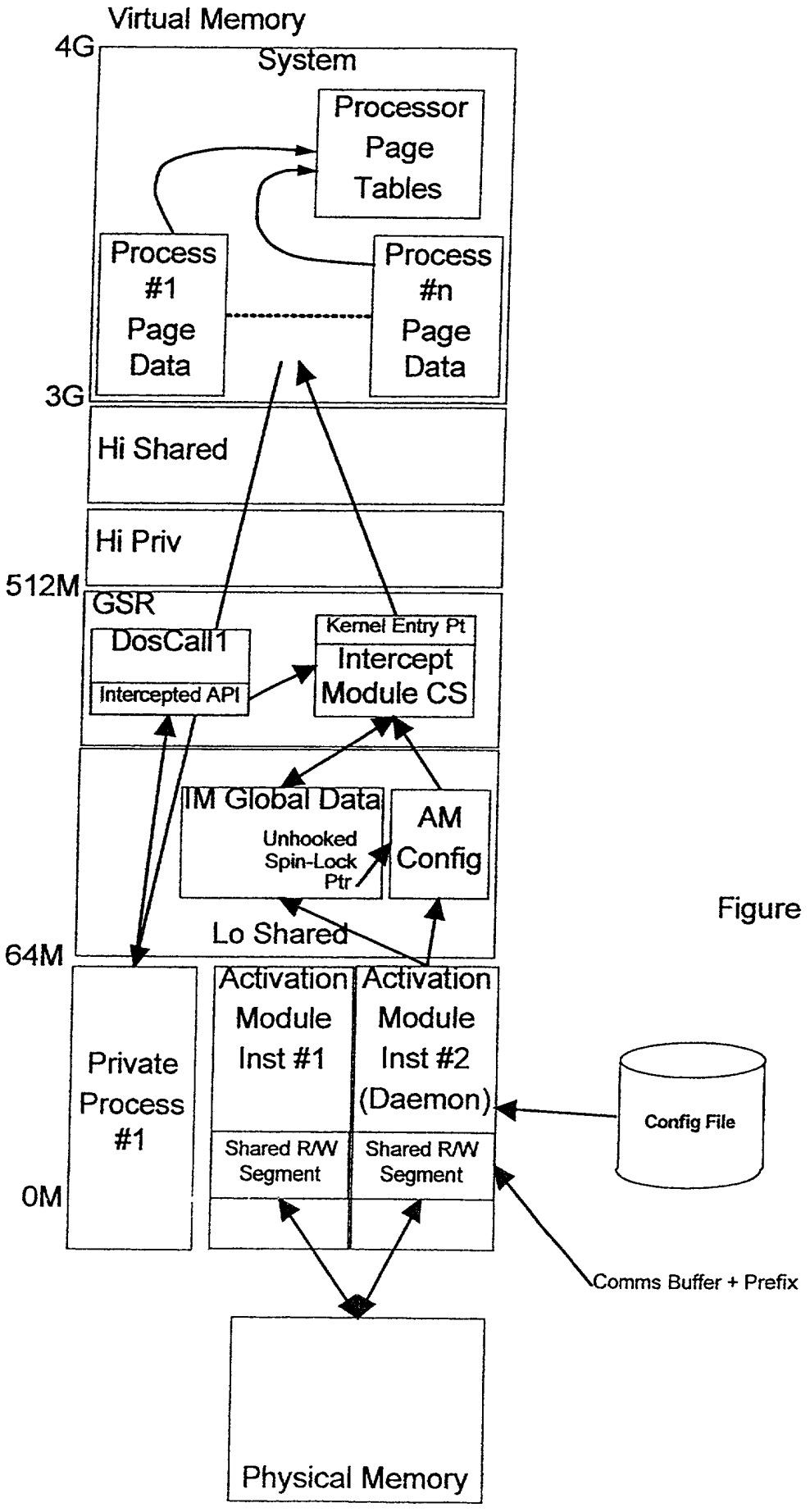
Virtual Memory
4G
System
Processor Page Tables
Process #1 Page Data
Process #n Page Data
3G
Hi Shared
Hi Priv
512M
GSR
DosCall1
Intercepted API
Kernel Entry Pt
Intercept Module CS
IM Global Data
Unhooked Spin-Lock Ptr
AM Config
Lo Shared
64M
Private Process #1
Activation Module Inst #1
Activation Module Inst #2 (Daemon)
Shared R/W Segment
Shared R/W Segment
0M
Config File
Comms Buffer + Prefix
Physical Memory

Figure 3

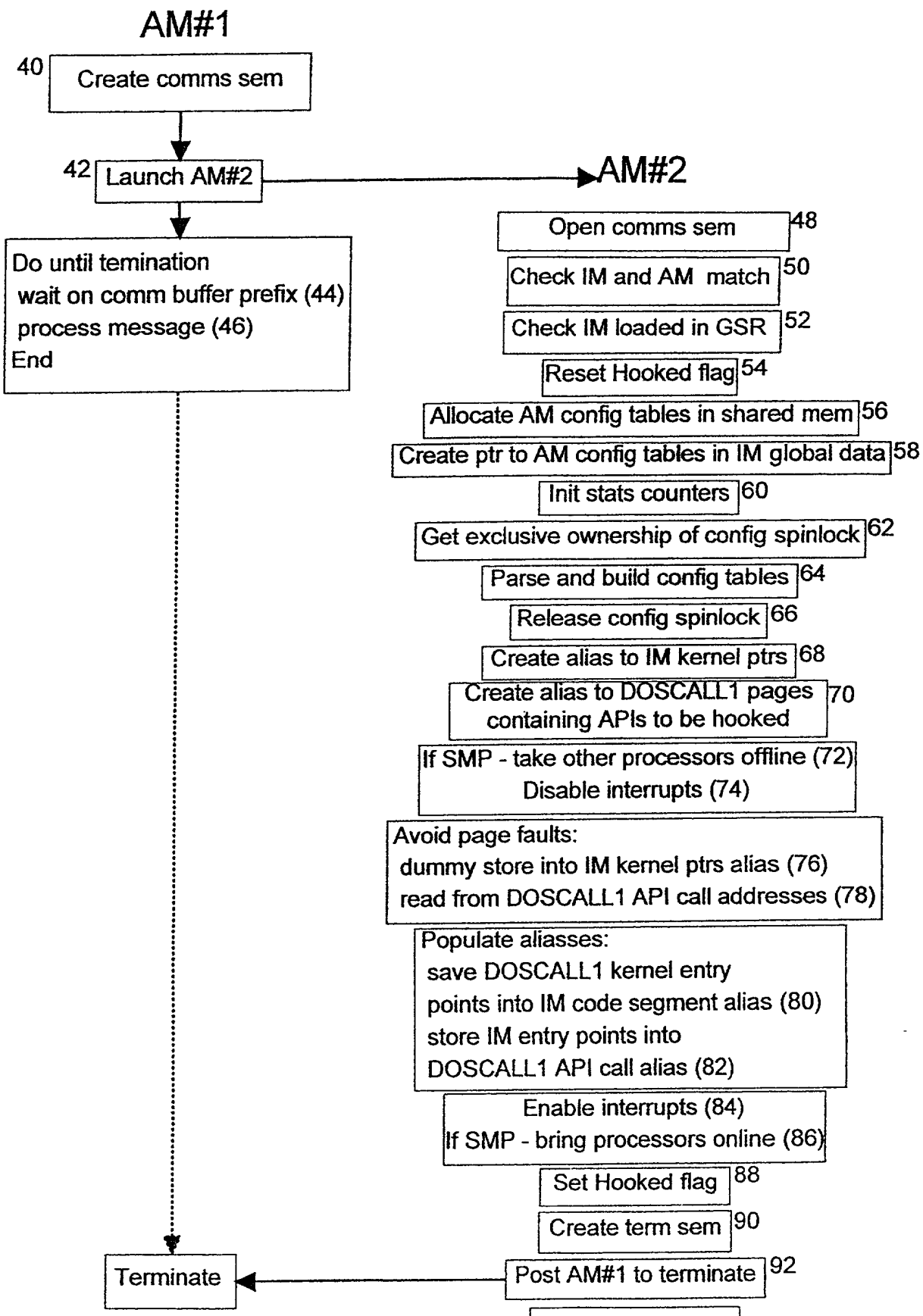
AM#1
40
Create comms sem
42
Launch AM#2
AM#2
Do until temination
wait on comm buffer prefix (44)
process message (46)
End
Open comms sem
48
Check IM and AM match
50
Check IM loaded in GSR
52
Reset Hooked flag
54
Allocate AM config tables in shared mem
56
Create ptr to AM config tables in IM global data
58
Init stats counters
60
Get exclusive ownership of config spinlock
62
Parse and build config tables
64
Release config spinlock
66
Create alias to IM kernel ptrs
68
Create alias to DOSCALL1 pages containing APIs to be hooked
70
If SMP - take other processors offline (72)
Disable interrupts (74)
Avoid page faults:
dummy store into IM kernel ptrs alias (76)
read from DOSCALL1 API call addresses (78)
Populate aliasses:
save DOSCALL1 kernel entry
points into IM code segment alias (80)
store IM entry points into
DOSCALL1 API call alias (82)
Enable interrupts (84)
If SMP - bring processors online (86)
Set Hooked flag
88
Create term sem
90
Post AM#1 to terminate
92
Wait on term sem
Terminate
Figure 4b

Figure 4a

Unhook IM:

```
If SMP - take other processors offline
  Disable interrupts
  Avoid page faults:
    read from DOSCALL1 call instructions
    read from saved IM kernel ptrs
  Reset aliasses:
    copy saved kernel ptrs to DOSCALL1
    call instruction aliasses
  Enable interrupts
  If SMP - bring processors online.
  Reset Hooked flag
Terminate
```

Figure 4b

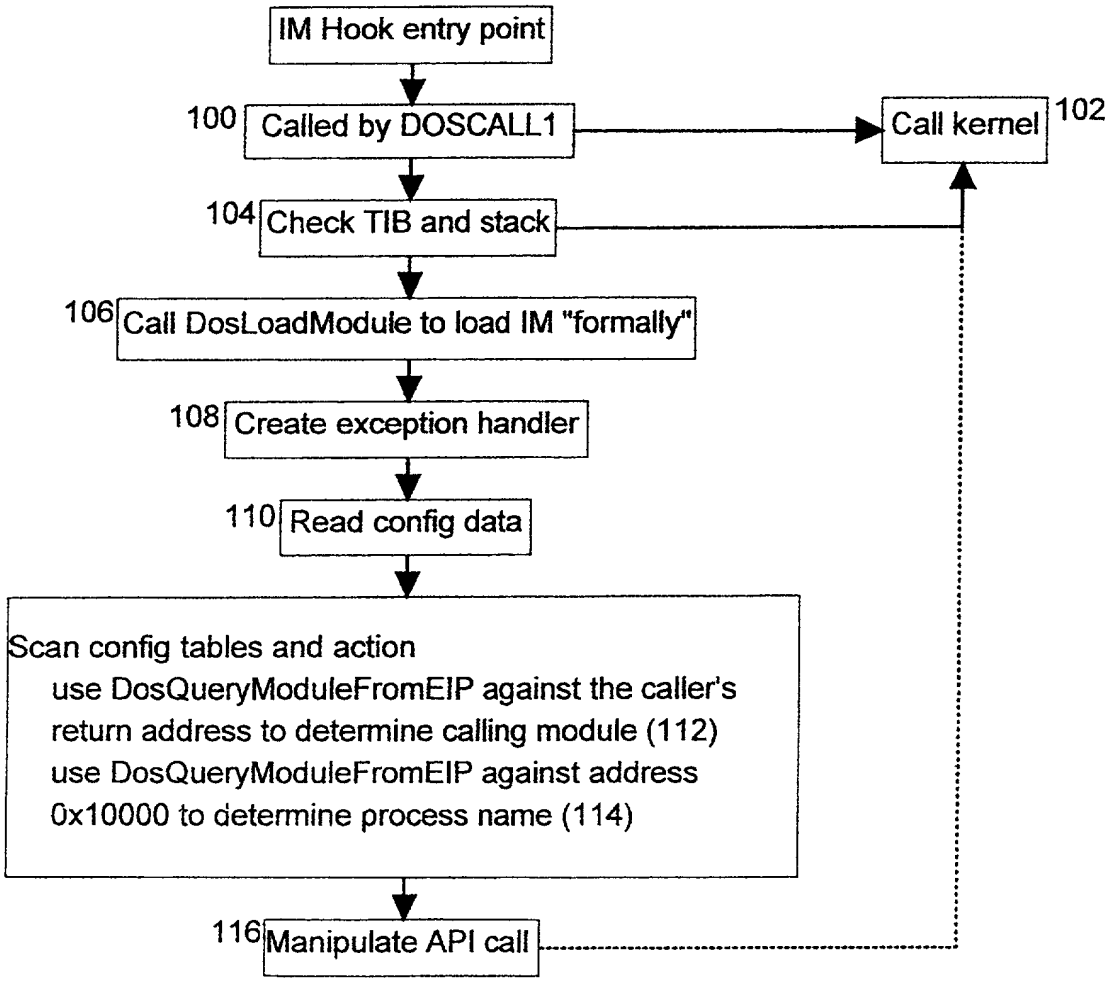

Figure 5